

Cyber Works/Maryland Tech Connection



A Public/Private Partnership for developing
a Next Generation Cyber Workforce

Before We Get Started...

- * Please mute your phone line.
- * Please use the chat function to ask questions to the presenter – we want to answer your questions!
- * The Presentation will be available after the Webinar.

Presenters

LeVorn Smalley

Cyber Industry Navigator, AAWDC

Christina Wiegand Majernik

Director, AoE Services

Frank Downs

Senior Instructor and Curriculum Developer, AoE

Agenda

- * Introductions
 - AAWDC
 - CyberWorks
 - TCS Cyber Intelligence Group
- * Purpose of Webinar
- * The Demand
- * The Threat
- * Overview of CyberWorks Training
- * Why and How to get Involved

Purpose of Webinar

- * Introduce **CyberWorks**, an initiative of the Anne Arundel Workforce Development Corporation (AAWDC), led by an industry-led Steering Committee
- * Discuss the demand for a trained Cyber workforce
- * Introduce a new program, sponsored by **CyberWorks** that combines technical training, an apprentice program and job placement/incumbent skills upgrade training

The Demand

- * From Fortune 500 companies to the Department of Defense, the demand for educated and experienced cybersecurity professionals has never been greater
- * More than 30,000 Cyber Jobs remain unfilled
- * The need for innovative solutions has never been more important

The Threat

- * Organizations are grappling with an aggressive threat environment on a daily basis
- * How do employers know that an individual has the required skill set to perform cyber functions within their organization?
- * In today's current cybersecurity certification construct, the answer has been a simple one: **They don't.**

Why?

Traditional approaches to training are not working:

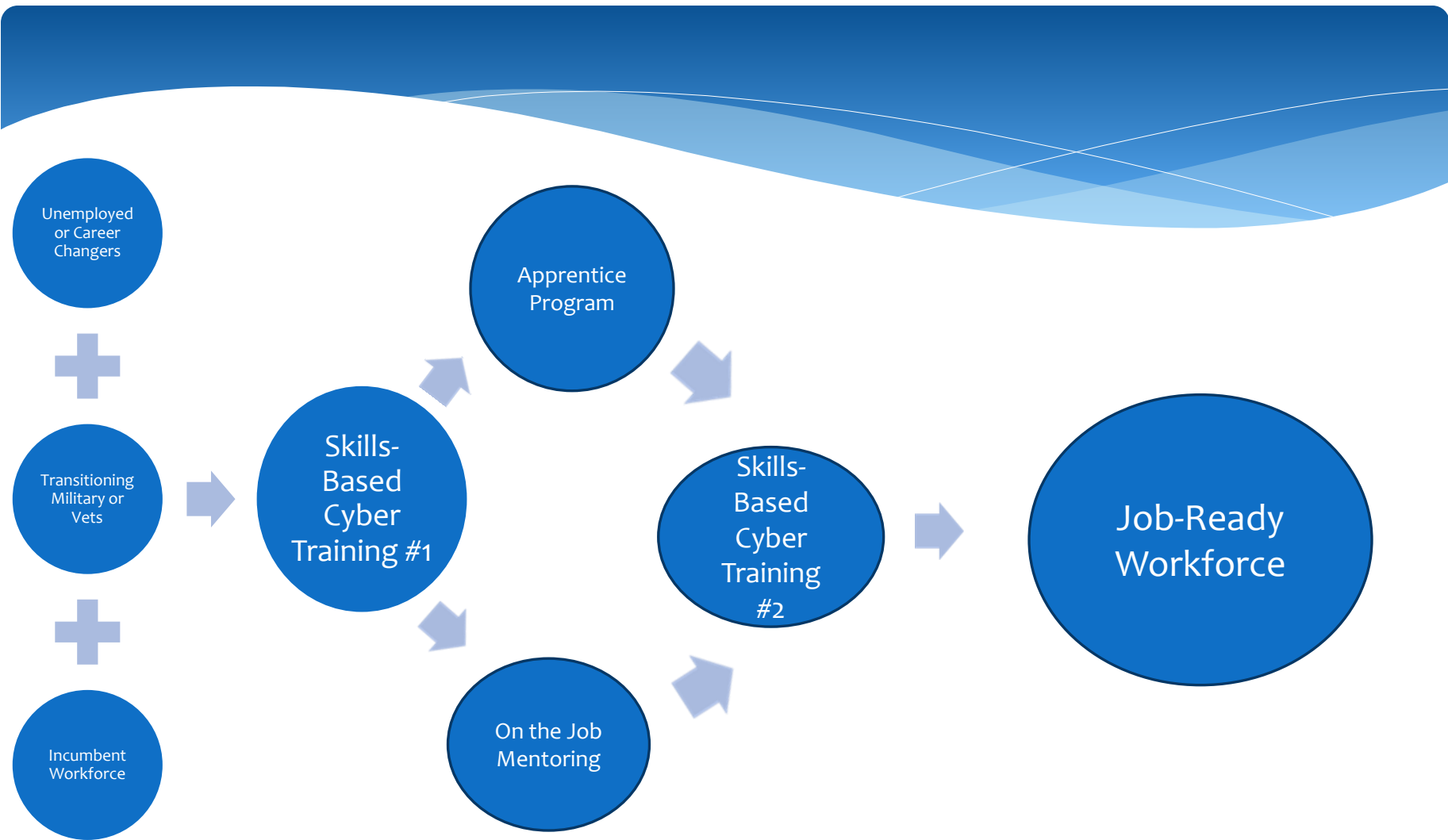
- * According to the [State of Cybersecurity: Implications for 2015](#), a joint survey published by ISACA® and the RSA® Conference, 82% of corporations expect a cyberattack in 2015; and **35% are unable to fill their open positions with qualified cybersecurity personnel**
- * Furthermore, **less than half of those surveyed believe that their current security teams have the ability to detect and respond to complex incidents**

A Solution

- * AAWDC has been a leader in addressing the Cyber workforce shortage in Maryland for the past 5 years
 - * **Pathways to Cyber** trained 886 individuals and was highly successful in meeting its objectives
- * But, the need for more experienced cyber workforce has emerged
- * **CyberWorks**, an industry-led initiative, funded by AAWDC and the Maryland EARN program is leading the way for a next generation workforce that will be job ready day one.

A Solution


- * The **CyberWorks** Steering Committee wanted to find a new way of approaching the demand through a new training program, coupled with a practical apprenticeship program that proves the skills gained in the training can be utilized in the workplace



CyberWorks = Training + Apprenticeship/On-the-Job Training Program

ISACA CSX: Next Generation Cyber Training

- * The Cybersecurity Nexus (CSX), is a new training program developed by AoE for ISACA - an independent, nonprofit, global association that develops and adopts globally accepted, industry-leading knowledge and practices for information systems.
- * CSX allows employers to recruit candidates with ***demonstrated*** cybersecurity competency and skills.
- * This next-generation training allows professionals to prove they have the technical skills and abilities to perform to cybersecurity job functions from **Day One**.

- 
- * Today, corporations need a baseline measurement of a candidate's skills against an actual network, one that measures knowledge of cybersecurity theories *and* required skills for job proficiency

ISACA CSX

NIST/NICE Framework

This is the first curriculum built upon the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Framework's Five (5) levels of cyber operational readiness:

- * **Identify:** Identification of threats and vulnerabilities
- * **Protect:** Protection of systems from outside threats
- * **Detect:** Detection of threats and system vulnerabilities
- * **Respond:** Response to, and mitigation of, cyber incidents
- * **Recover:** Recovery from incidents and disasters

ISACA CSX

NIST/NICE Framework



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy



PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology



DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process



RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements



RECOVER

- Recovery planning
- Improvements
- Communications

ISACA CSX

Globally Accepted Standards

CSX certifications are founded upon globally accepted standards and frameworks: the **NIST Framework** for Improving Critical Infrastructure Cybersecurity, **NIST SP 800-53** Revision 4, the **ISO 27000 series**, and **COBIT 5**.

Each level of CSX certification requires increasing levels of demonstrated competency — with scenarios growing in complexity and sophistication.

ISACA CSX

- * **CSX Practitioner**—Demonstrates ability to serve as a first responder to a cybersecurity incident following established procedures and defined processes.
 - 3 training courses
 - 1 certification
 - prerequisite for CSX Specialist

- * **CSX Specialist**—Demonstrates effective skills and deep knowledge in one or more of the five areas based closely on the NIST Cybersecurity Framework: Identify, Detect, Protect, Respond and Recover.
 - 5 training courses
 - 5 certifications
 - requires CSX Practitioner

CSX P

The CSX Practitioner will be a first tier incident responder with the following competencies:

- * Utilize vulnerability assessment processes and associated scanning tool sets to initially identify and document vulnerabilities, based on defined asset criticality and technical impacts.
- * Obtain and aggregate information from multiple sources – for example: logs, event data, external intelligence – for use in threat intelligence, metrics and incident detection
- * Implement specified cybersecurity controls – for network, application, endpoint, server, and more – and validate that controls are operating as required
- * Conduct ongoing control tests and validations to verify effectiveness of controls and identify deficiencies and vulnerabilities

CSX S



Identify: Identification of threats and vulnerabilities

Protect: Protection of systems from outside threats

Detect: Detection of threats and system vulnerabilities

Respond: Response to, and mitigation of, cyber incidents

Recover: Recovery from incidents and disasters

Get Involved!

Why Partner with CyberWorks?

- * ***Help grow your Cyber workforce!***
 - * Cultivate new cyber talent with the right skills and ready to perform on day one
- * ***Help grow the Cyber workforce in the State of Maryland!***
 - * Despite the universally recognized need for highly skilled cybersecurity professionals, tens of thousands of cybersecurity jobs remain unfilled.
 - * The greatest impediment to an effective defense against cyber threats is this severe deficiency of qualified, skilled professionals.

Get Involved!

Why Partner with CyberWorks?

- * Provide a continuum of on-the-job training by placing candidates immediately into a paid **apprentice** program and exposing them to an operational environment in corporate Security Operations Centers and IT security environments.
- * **This benefits candidates and employers to meet hard to fill positions!**

Get Involved!

Why Partner with CyberWorks?

- * *Skills upgrade training for your incumbent workforce*
 - * In an RSA report released in May 2015, less than half of those surveyed believe that their current security teams have the ability to detect and respond to complex incidents
 - * There are many companies throughout the State of Maryland that would benefit tremendously from an incumbent worker training program, providing their existing employees the requisite skills to defend their employer's most critical asset

Aggressive Goals

- * Train new and incumbent workers over the next three years in critical, job-ready cyber skills
- * Define a new cyber apprentice program
- * Commitment from partners to hire new workers as apprentices
- * Lead a new way of thinking about job-skill readiness!

Pre-requisites/Prior Experience

Optimal pre-requisites include the following:

- Computer Fundamentals (CompTIA A+)
- Network Fundamentals (CompTIA Net+)
- Security Fundamentals (CompTIA Security+)
- Windows and Linux Fundamentals, or
- Prior military training.

Prior military training includes:

- Navy/Marines: CTN/ITA, JCAC, 6694, 0651, 0652, 0653, 0656, 0658, 0659, 0681, 0689, 2651, 2611;
- Army: 25 series and 35 Quebec;
- Air Force: IN

Upcoming Training

Co-Hort #1:

CSX P Training

- * Week 1: July 27-31
- * Week 2: August 3 – 7
- * Week 3: August 10 – 14

Apprentice Program

2 CSX S Training Programs

- * Week 1: November 2 - 6
- * Week 2: November 9 - 13

How to Get Involved

For companies that want to take advantage of this program, the company must:

- * Be a Member of CyberWorks and/or Maryland Tech Connection Consortium
- * Submit Business Questionnaire
- * Sign Letter of Intent
- * Agree to Contract Terms
- * Engage in Employee Cultivation

Points of Contact

LeVorn Smalley, Cyber Industry Navigator
lsmalley@aawdc.org
CyberWorks Partners and Candidates

Christina Wiegand Majernik, TCS
cwiegand@telecomsys.com
Incumbent Worker Training